ProtectUK

Tactic RB2: Ensure full adherence to incident response and business continuity planning checklist

ProtectUK publication date
14/12/2023

Information and Intention

Incident response and business continuity planning are essential for organisations. They set out how the business will respond prior to, and operate following, an incident and how it expects to return to 'business as usual' in the quickest possible time.

Ensure your Business Continuity Plans are in place with understanding of and adherence to Incident Response and Business Continuity Checklist. It need not be specific to terrorist incidents and can apply to any major disruption such as fire, flooding or power fault.

An Incident Response Plan is a plan of action for the efficient deployment and coordination of services, agencies and personnel to provide the earliest possible response to an emergency.

The following websites are useful for advice and training on resilience:

- Emergency Planning College
- Business Emergency Resilience Group
- Cabinet Office
- Government Emergencies, Preparation, Response and Recovery
- Government Emergency Planning

Crisis management is about your arrangements to manage strategic, complex and unprecedented events. It is rarely standalone and will require integration with other disciplines. An incident may require a Crisis Management Response without the need for a Business Continuity Plan activation. This may be, for example, in the event of major negative media attention about the business.

In contrast, there may be a 'creeping/rising tide crisis' where a disruption, such an attack on an IT

system, emerges and, if not managed effectively, turns into a crisis. The incident response arrangements must therefore be flexible enough to manage both an operational disruption, which may need to be escalated, and a crisis situation, which requires strategic leadership.

Method

In order to ensure full adherence to the Incident Response and Business Continuity Planning checklist, organisational behaviour must be positively influenced in ways that will enhance the security culture.

This can be achieved by regularly reviewing and exercising your plans to make sure that they remain accurate, workable and up-to-date. Additionally, consider reviewing plans if there is an attack elsewhere, or there is a change in threat or circumstance including to suppliers, contractors or stakeholders.

Through training, make sure staff understand their personal responsibilities, accept the need for security measures and that security is seen as part of everyone’s responsibility; security is not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations. Rehearsals and exercises should, wherever possible, be conducted in conjunction with all partners, emergency services and local authorities.

Managing risk and security planning are on-going processes. Part of the validation process is to exercise plans and use any learning to further refine and make sure plans are workable to achieve the required outcomes.

The aim of your exercises should be to:

- Make sure that plans work (verification).
- Develop staff and third-party competencies and enable them to understand and practice carrying out their roles within the plan (training).
- Test established procedures to make sure they remain valid (exercise, rehearse and validate).
- Provide learning to further refine the plan (review).
- Regularly review aspects of your Incident Response and Business Continuity Planning checklist, ensuring each element remains valid.

Administration

Policy and procedures should mention adherence to the Incident Response and Business Continuity

Planning checklist should the threat level be raised or following an incident.

Identify ownership of the incident and governance of the decision making, including who is responsible for the management, coordination and strict compliance, together with the relevant records keeping, and how its effectiveness is assured.

Ensure staff understand processes and procedures to be adopted, including action and contingencies (e.g. mail handling, courier deliveries, receiving of visitors etc.).

Risk Assessment

Regarding protective security and resilience, the best way to manage the hazards and risks to a business is to start by understanding and identifying the threats, vulnerabilities and the resulting business impact.

This will help to answer:

- What protective security and resilience improvements need to be made.
- What type of security and contingency plans need developing.

For some venues and public spaces, simple good practice, coupled with staff vigilance and well exercised contingency arrangements may be all that is needed. If, however, an assessment states the presence of an attack vulnerability, appropriate protective security measures should be applied to reduce the risk to as low as reasonably practicable.

A key action for a business is to create a Crisis Communication Plan (TACTIC EB4). This should be a core component of its risk preparations. It should be developed following a detailed risk analysis looking at potential issues and possible solutions.

Typically, these issues relate to an organisation’s people, assets, property and operations, and the plan is there to guide action and communications.

Communications

Internal Stakeholder Engagement:

Certain aspects of your Incident Response and Business Continuity Planning may not necessarily be communicated to all your staff. However, staff members should be briefed on what to do in order for them to adhere to the Incident Response and Business Continuity Planning checklist. All security management/security staff should understand their role and function when it comes to adherence of the checklist.

It is necessary to ensure points of contact regarding this action are known to staff internally, and partners externally. Any information regarding adherence to Incident Response and Business Continuity Planning checklist should be disseminated internally through the Communications function.

Internal communications should also encourage a positive security culture and security awareness by general staff.

You must provide regular information for your staff so that they can help deliver on the security plan. Your internal audience will inevitably cross over into your external audience, so you should consider the messages you want them to convey to their external networks, e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Engagement with neighbouring businesses should be on a regular basis and should be constructive. However, you may decide to keep sensitive parts of your Incident Response and Business Continuity Planning within your own organisation.

Early identification and engagement with key external stakeholders is important. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering on any security outcomes, and consideration should also be given to engaging with any working groups or forums who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.
- Communications should be genuine and timely, s there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

External Media Engagement:

After a terrorist incident has occurred, organisations should not communicate directly with the media

or external audiences on anything related to the incident, without prior consultation and agreement with the police. In addition, avoid revealing details about the incident through social media without prior police consultation.

An appropriate individual should be identified in the organisation to liaise with the police in order to disseminate approved information which is accurate, and which will not compromise the criminal investigation.

Health and Safety/Other Legal Issues

Businesses/organisations that seek adherence to their Incident Response and Business Continuity Planning checklist should ensure that all activities are assessed in line with Health and Safety and other legal/policy frameworks, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- Employment Rights Act 1996

Your actions must be justified, necessary and proportionate to the threat you are facing.

Adherence to the Incident Response and Business Continuity Planning checklist must include consideration of details of your organisations insurance policies. Consideration must be given regarding the personal health and safety of all staff in the performance of their duties.

There must be well defined governance arrangements and records must be kept of the issues, decisions made, and the reasoning behind these decisions.

Records will provide evidence to any investigations, coroners' inquiries and public inquiries and assist in defending against legal action, criminal charges or civil claims. The importance of keeping accurate records and having well defined governance arrangements has been demonstrated during the Manchester Arena Inquiry.

KEYWORDS
BUSINESS CONTINUITY
CRISIS MANAGEMENT

ATTACK

INCIDENT MANAGEMENT

INCIDENT RESPONSE